Set Task Electronic Template – Unit 11

Task B - Activity 4 Template: Forensic Incident Analysis

*Use the section headings below to structure a response for **each** evidence item.*

Evidence item:
Method of acquiring the evidence:
Evidence detail:
Evidence reliability:
Conclusions:

After all the evidence items, provide an overall conclusion.

Evidence item: Baljinder's account
Method of acquiring the evidence: Hypothetically this would be obtained through observations and conversations while working for BCTAA.
Evidence detail: Missing items include: Surface Pro 3 laptop, Samsung Edge S5 phone, 3 x USB memory sticks, various sizes and makes, 3 x wireless mouse and 2 x wireless keyboards. Over the bank holiday weekend people left at lunch and the area was left empty at 14:00. Items were left out in informal seating and work area. Nothing noticed until Tuesday afternoon when laptop was booked for meeting. The search for it made them realise other devices were missing. Uncertain of when items disappeared. EH Management Company said other incidents occurred over bank holiday weekend.
Evidence reliability: Good as the scenario shows that the informal seating and work area are just after controlled doors.
Conclusions: The fact that items were left in informal seating and work area implies that they were left out in obvious places. Therefore all it would have took is for someone to gain access pasty controlled doors after 14:00 when everyone had left.

Evidence item: Summary of meeting with the EH management company
Method of acquiring the evidence: Baljinders notes rom a meeting with senior management.
Evidence detail: Wages and conditions are deliberately better than those of similar jobs ion the area, this reduces staff turnover and encourages loyalty. Previously very few dismissals for dishonesty and none this year. Number of picoting and opportunity thefts reported on Friday in restaurant shop and bar areas. Extremely busy and CCTV footage was inclusive. Shops reported problems with customer have phantom charges applied to contactless payment cards. Phantom charges have happened in past due to system errors. Both BCTAA and the recruitment company reports thefts, without evidence of forced entry over the bank holiday weekend. Recruitment agency lost some small electronic items from its reception area.
Evidence reliability: Good as they come straight from the meeting with senior management and would be serious about this incident.
Conclusions: The information confirms that there were intruders in both floors with BCTAA and Recruitment Company so it was an organised attack. In addition reported thefts from the restaurant imply that there were thieves in the area who could have been the intruders.

Evidence item: Door access control logs
Method of acquiring the evidence: Door access control log with card entry details
Evidence detail: entries 14, 15, 16 and 17 all had correct cards however the cardholders claimed either they didn't attempt to gain access or they cant remember

if they used the card or not. Party was happening on 20th floor which BCTAA staff were present at including BCTAA senior manger whose card gained access to 19th floor and he claimed he didn't use it.
Evidence reliability: Very reliable data control log cannot be tempered with.
Conclusions: Clearly it seems unauthorised access to the 19th floor was gained around the same time of the part on the 20th floor when the senior manager claimed he was at while his card was used to gain entry to 19th floor. This might imply that thieves from the 20th floor could have taken and used his card while he was at the party.

Evidence item: Network diagram
Method of acquiring the evidence: This would hypothetically be part of the BCTAA IT documentation.
Evidence detail: The diagram shows connections to the electronic door control system and staff devices.
Evidence reliability: Good as there is no reason to believe that the network was altered from the diagram that is shown.
Conclusions: This evidence isn't very significant as the attack was more of a physical entry.

Evidence item: Laptop tracking report
Method of acquiring the evidence: App called "Find my device" received notification.
Evidence detail: The location of the laptop a week late is now Nairobi, Kenya.
Evidence reliability: Good as the device is updated periodically when it's connected to WI-FI and the location is believable from where it has transported within a week.
Conclusions: The laptop being at such a distance away suggests that the laptop was sold on and transported to Kenya for a profitable fee.

Evidence item: Cyber security documentation
Method of acquiring the evidence: Incident management policy
Evidence detail: The team consists of the network manager, senior BCTAA manager present at the time of the incident and the BCTAA public relations officer. The policies go through a list of required protocols which must be actioned when theft of IT equipment occurs.
Evidence reliability: Good as it is a company policy it doesn't vary unless company deem it appropriate.
Conclusions: following this company policy it seems that all these actions are handled in the best possible way to identify why, where, how and who stole the IT equipment and how to best avoid it in the future.

In conclusion I believe that the most likely explanation is that while the BCTAA party was taking place on the 20th floor at the restaurant and bar where there had been reports of thefts and pickpocketing in the same day, is where the senior manager had his card pickpocketed. After his card was pickpocketed the thieves used it to gain access past the controlled doors into the informal seating and work area where the devices were unprofessionally left out. The senior manager said that they were certain they didn't try to gain access and that they were at the party on the 20th floor however the door access control log shows that their card was in fact used to gain entry to the 19th floor where the devices were left out. After the devices were taken they were sold and exported to other countries such as Kenya. Overall I believe this is the most feasible explanation and the evidence clearly represents that.